PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 12/14

A1

(11) International Publication Number: WO 92/12485

(43) International Publication Date: 23 July 1992 (23.07.92)

(21) International Application Number: PCT/US91/09270

(22) International Filing Date: 10 December 1991 (10.12.91)

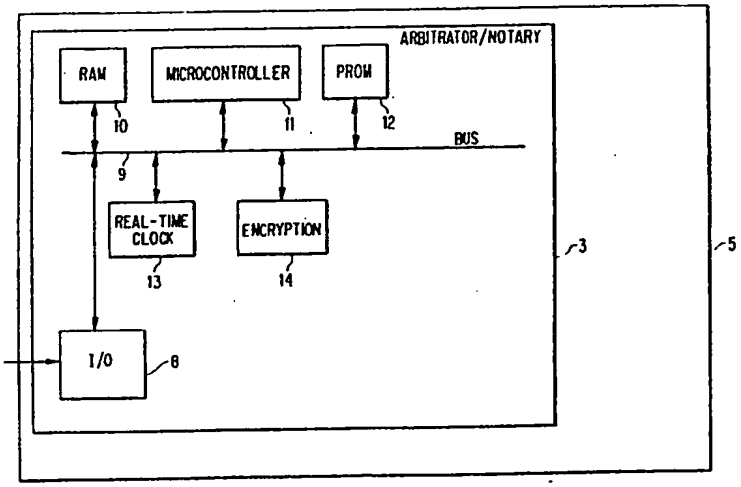
(30) Priority data:
637,675 7 January 1991 (07.01.91) US

(71)(72) Applicant and Inventor: BLANDFORD, Robert, R. [US/US]; 1809 Paul Spring Road, Alexandria, VA 22307 (US).

(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, KR, LU (European patent), MC (European patent), NL (European patent), SE (European patent).

Published
With international search report.

(54) Title: DEVICES TO (1) SUPPLY AUTHENTICATED TIME AND (2) TIME STAMP AND AUTHENTICATE DIGITAL DOCUMENTS



(57) Abstract

A digital system, called a notary, designed to (1) provide authenticated time and/or (2) to time stamp and authenticate digital documents, comprising a clock and digital circuits. The clock uses a power-supply system designed to avoid failure, and the notary stops functioning should any failure of the clock or power source be detected. The time and/or document is authenticated by a secret key in the digital circuit which is inaccessible from outside the notary. The system is sealed so that the clock time may not be changed or the secret key discovered without detection. The security and usefulness of the system rests on the integrity of this seal. A user may supply a digital signature and sequence number to be authenticated so that it may later be verified that the user archived the document at the time stamped so that missing documents in a file may be identified. The notary also may supply an identification number and sequence number to be authenticated with the time and/or document to identify the notary and to detect deletion of documents and/or possible excessive use of the notary. A mode of operation of the notary is available in which it computes a standard format of a document before authentication so that copies of the document made by different methods, e.g. handwritten facsimiles, may also be authenticated. The system may be used in conjuction with a computer to ensure that the computer is booted with the correct time. Using either private or public key techniques, the time and/or documents may be verified without direct access to the secret key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	RU	Russian Federation
CG	Congo	KP	Democratic People's Republic of Korea	SD	Sudan
CH	Switzerland			SE	Sweden
CI	Côte d'Ivoire	KR	Republic of Korea	SN	Senegal
CM	Cameroon	LI	Liechtenstein	SU	Soviet Union
CS	Czechoslovakia	LK	Sri Lanka	TD	Chad
DE	Germany	LU	Luxembourg	TG	Togo
DK	Denmark	MC	Monaco	US	United States of America

DEVICES TO (1) SUPPLY AUTHENTICATED TIME AND (2) TIME STAMP AND AUTHENTICATE DIGITAL DOCUMENTS

BACKGROUND OF THE INVENTION

This invention relates to devices and means, at least partly in hardware (1) to provide authenticated time to a computer or other user; and (2) to assure that a specified digital document did in fact originate with a particular person and was stamped at a particular time and in a particular order by a particular device (the "arbitrator" or "notary");

In recent years there have been many articles in the trade and popular press describing incidents in which computer records have been erased or altered illegally.

Computer records are particularly liable to such alteration; they can be less secure in this respect than are paper records because an altered paper record may reveal erasures. Even if a paper record is created from scratch, the age of the paper or ink on a single sheet of paper, or progressively in a bound notebook, may reveal the forgery. Such aging does not occur for computer records. And, of course, handwriting or other forensic analysis may reveal that a paper document was signed by other than the nominal author.

Even permanent records on such WORM devices as optical disks may be read and re-written, possibly with falsified dates, on a fresh disk after making desired alterations.

This, and many other falsification techniques available, for example, to a superuser or other "owner" of a computer system would be made more difficult if all computers were required by hardware to access an authenticated source of time in order to set the system clock.

From a positive point of view, it would be desirable if computer records could take the place of paper records for legal purposes, thus minimizing the large volume of stored paper.

As another use, a person keeping a diary would like to be sure that the record, once committed to the permanent computer recording device cannot be undetectably altered, even by himself.

In these cases it may be important that archived records be traceable to the person who actually created them, that the records be unaltered, unalterably time-stamped and sequenced, that it be clear which physical device (the "notary") actually performed the time stamping and authentication, and that access to the records be controlled by passwords and other means.

It would also be desirable if paper copies of the original digital records could be certified as authentic; i.e. that it could be verified that each copy was archived by a particular person on a particular machine at the indicated time. It would also be desirable if it could be shown that no documents are missing from a nominally complete file of the paper records.

In the present invention these goals are achieved by the use of a sealed digital processing circuit, called an arbitrator (or "notary"), which contains a real-time clock which either can not be reset, or can be reset only under strict procedures, and an authentication circuit which can compute digital signatures using a secret key, inaccessible from outside.

For the purpose of (1) providing authenticated time, the first aspect of the invention, the arbitrator computes an authentication check (signature) over the time from the sealed clock and the arbitrator's identification number (ID) and upon request returns the time and signature to the user. If the signature was

computed using private key techniques then the user or other verifier may validate the signature by recomputing the signature with a supplemental device which also contains the secret key in an inaccessible form. This would, of course, be preferable to allowing the user to have direct access to the secret key, since this would enable him to falsify the signature. Many other methods for generating and validating signatures using private keys may be found in the open cryptographic literature.

If the signature of the time and ID was computed using public key techniques then the verification of the signature may be performed using the public key without any form of access to the secret key.

In some applications the user may want to ensure that the time and authenticating signature received is not simply a copy of a previous message. This can be assured by the user generating and sending to the arbitrator a random number which the arbitrator then appends to the time from the sealed clock before computing the digital signature. The signature then verifies that the time was not authenticated before the random number was generated.

For the purpose of (2) authenticating documents, a second aspect of the invention, the arbitrator computes a signature over the full text of the document (or in some cases preferably of a hash of the full text of the document), a sequence number provided by the user, the user's digital signature, the internal clock time, the arbitrator's ID, and the arbitrator's sequence number. The arbitrator then returns this signature to the outside where it can be verified using the public key and compared to the original.

In order to provide background information so that the invention may be completely understood and appreciated in its proper context, reference is made to a prior art patent application and to a publication in methods of time-stamping digital documents as follows:

U.S. Patent Application Serial No. 07/375,502 by Blandford discloses a digital system in which an arbitrator time stamps digital data records, and computes an authentication check (signature) on the data plus time using a key inaccessible from outside of the system. The system then stores the data, time, and authentication check on a secure memory storage device. The complete system is sealed so that the clock cannot be surreptitiously reset, and the clock is provided with non-stop power. The Application discusses how even if the digital records are later copied from the memory storage device the digital signature can be used to certify that the record was recorded at the specified time on the particular system.

Of course the security this of arbitrator system rests largely on the degree to which the sealing means cannot be subverted. Should this be possible the clock could be reset and/or the secret key discovered, resulting in the possibility of forgery.

An article in "Advances in Cryptology--Crypto '90," Springer-Verlag, LNCS by Stuart Haber and W. Scotte Stornetta entitled "How to Time-Stamp a Digital Document" discloses means for a central Time Stamping Service (TSS) to time-stamp documents submitted to it by different users. "Reliable" time is achieved by means quite different from the use of the sealed, non-resetable clock discussed above. On the other hand the basic motivation to provide document authentication from calculation on a "reliable" time stamp and the digital document itself, is similar to that of Blandford and of the present application.

In their first approach, Haber and Stornetta achieve the time stamping by computing a digital signature on a hash of the document, plus the users ID, plus the time, plus a sequence number assigned by the TSS, plus information linking this request to the previous one (the time, ID, and hash of k previous users).

(Haber and Stornetta discuss cryptographically secure one-way hash functions (hereafter referred to simply as a "hash") and provide a reference to a practical source of such functions.) The TSS also eventually provides the user with the IDs of k subsequent users. The time information is thus constrained to be approximately authenticated by the fact that the user, or some other verifier, could later consult the users previous and subsequent to the document in question and check that the publicly authenticated times and hashes do constrain the time and message.

In their second approach there is no TSS; the user simply sends the hash out to a carefully randomly selected set of authenticators; they append the time from their own clocks and return a set of authenticated signatures.

Both of Haber and Stornetta's approaches are vulnerable to collusion on the part of a set of users; especially, for example, in the case where the network of users is all in a single institution under a single system manager, e.g. a single large manufacturer, or government agency, or insurance firm. Basically the unlikelihood of this collusion must be balanced against the unlikelihood in the present application of being able to clandestinely break the seal on the arbitrator and undetectably alter the clock or determine the secret key.

Also, since they require timely access to a communication system and to one or more cooperating and reliable computer systems, the approaches of Haber and Stornetta are unsuitable for an isolated system such as the typical personal computer or portable "diary" or to "secure" users which would prefer to have no contact with outside users.

Of course it would be possible to combine the strengths of the two different approaches to providing authenticated time by providing Haber and Stornetta's TSS, or each of the users in their hypothetical network, with a source of secure, authenticated time as discussed by Blandford and in this application.

Whatever the precise merits, features and advantages of the above cited references, none of them achieves or fulfills the purposes of the present invention.

SUMMARY OF THE INVENTION

It is an object of the first aspect (1) of the present invention to provide a device which can provide authenticated time to any client; and it is a second object to provide means to ensure that a computer making use of this device cannot be booted with an incorrect time.

The first object may be achieved by sealing together in a single package a digital real-time clock and an encryption circuit with a secret key which is inaccessible from outside the system. The seal should be tamper-proof so that a breach of it is apparent upon inspection and so that a breach of the seal will cause the system to permanently cease operation. The overall circuit may be referred to as the arbitrator.

The clock is to have a power supply designed to provide continuous power for the useful life of the system. The clock is also to be designed to be non-resetable, or to be non-resetable without execution of a carefully prescribed procedure, and the arbitrator is to shut down should the power supply to the clock fail or should some other system diagnostics fail. In some realizations it might be useful to allow the clock to be re-setable and for the arbitrator to restart so long as a permanent, accessible record of the starting and stopping were kept in non-volatile memory within the sealed arbitrator. It would be useful if access to different functions of the arbitrator were controlled by password or other similar means.

This source of authenticated time can be used to achieve the second object, that a computer system cannot be booted with the incorrect time. This is done by

providing that a critical element, an element without which the computer cannot operate, of the computer is sealed together with the computer clock and with a circuit which can generate and output a large random number and which can verify the digital signature computed over the random number, the time, and the ID provided by the authenticated time device. This seal should have the same properties as that of the arbitrator itself. (The source of authenticated time could, of course, be within the computer itself; and could even be the computer clock itself and be sealed together with the critical element of the computer. In this latter case, however, there would be no need for encryption; the computer would simply always get its time from the un-resetable sealed clock.)

The computer clock is started and the computer booted up only if the time can be verified to have come from a source of authenticated time. If public key techniques are used then there is no need to make the public key within the computer inaccessible; with many private key techniques the key in the computer would have to be inaccessible to eliminate the possibility of falsifying the time. To ensure that a previously recorded time and signature was not being resubmitted to the computer, the system sealed within the computer could generate a random number and send it to the arbitrator which would then append it to the time and arbitrator ID before calculating the signature and returning it to the computer. The computer could then be sure that the time did not originate before the random number was generated.

It is an object of the second aspect (2) of the present invention to provide a device and means which can authenticate the author, text, time, and time stamping device (arbitrator or notary) of a digital document, and which ensure that one or more digital documents cannot be removed from a sequenced file of such documents without that fact being apparent.

This object may be achieved by adding to the capability of the arbitrator discussed above the capability of observing data arriving from the user and of computing the signature over that incoming data (or in some embodiments a hash of that data) together with the authenticated time and the arbitrator ID. In addition to the document data the incoming data would include the user's digital signature, previously computed by the user over the document data, or hash of the document data, and the user's sequence number. Again, the user's signature in the authenticated document could be verified either by public or private key techniques.

If the full document data were presented to the arbitrator, the signature could be computed either over the complete document, or the arbitrator could first compute a hash of the document and compute the signature only over the hash plus the user's signature and sequence number, the time, and arbitrator ID and sequence number. If the user had already performed a hash on the original document, an additional hash would be unneeded. Perhaps no hash would be computed for data below some fixed number of bits. The final digital signature is presented to the user at the output ports of the arbitrator. The arbitrator might also make available to the user at the output ports the original data so that the user could compare the data sent with the data returned in order to verify that the signature had been derived from the specified data.

Note that if a user should choose to append consecutive sequence numbers to the text of each document that he requests to be authenticated and which he then places in a particular file, then it will be possible for a verifier to check if documents have been removed from the file simply by looking for numbers missing in the sequence. Because of the authentication of the sequence number and date it would be impossible, even for the owner, to erase a document and then adjust the subsequent sequence numbers in the file without also changing all the dates. Similarly a document could not be changed without

also changing the date to a later date, which may well have to be later than that on the following document in the file. Of course this last benefit is obtained whether or not there is a sequence number.

The arbitrator might usefully have a mode of operation, if presented with ascii text, in which the authentication is calculated only after the document text has been transformed to a standardized, but still readable, format, e.g. with one space between all words and symbols, no tabs or new lines, and with data in unusual formats, e.g. scientific formulas, omitted from consideration. Obviously, transformations which would reduce formulas, tables, special fonts, etc. to a standard form are also possible. (Complex documents, e.g. digital pictures, if they are to be recognizable, would have to be archived in their original digital form in order to be verifiable.) In this way a conventional ascii document could be verified even if it had previously been copied in ways such as retyping or even cursive transcription, which altered the paragraph or word spacing format.

It could also be useful, for the notary itself to append and authenticate its own sequence number to each document. This could be useful in cases where a single user did not append his own sequence number. It could also be useful if there were only a few users of the notary so that a document could be found to be missing from one user's files by examination of the files of all of the other users.

This completes the summary of the invention; it can be seen that the invention has been presented in two aspects, the later aspect is an enhancement of the first.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a block diagram representation showing the relationship of the components of the system which supplies authenticated time. It also serves as a block diagram representation for the system which supplies authenticated time, author, notary and sequence for digital documents.

DETAILED DESCRIPTION

The preferred embodiment of the aspect of the present invention a system (1) which will supply authenticated time will now be described by reference to Fig. 1.

In Fig. 1 we see that the time source or arbitrator 3 is comprised of a random access memory (RAM) 10, some part of which is non-volatile e.g. EEPROM, a microcontroller 11, programmable read-only memory (PROM) 12, a real-time clock 13, and an encryption circuit, 14. The arbitrator also has an I/O circuit 8, by means of which the arbitrator may, under control of the microcontroller 11, observe the state of the external communication lines and by means of which data may be presented by the microcontroller 11 to the external communication lines. Communication between the microcontroller 11 and the other devices is carried out via a microprocessor bus 9.

All of the above components are packaged or sealed in a manner which makes them and their stored data physically inaccessible without making such an intrusion apparent upon inspection and causing the arbitrator itself to permanently cease operation. The arbitrator could be assembled as a conventional chip set and encapsulated with a tamper protection system 5. Or, in the preferred embodiment, it could be manufactured as a single chip package built so that any attempt to probe the system, for example to determine the secret key, would in fact destroy the information. This could be accomplished with a combination of piezo-electric drives (to destroy the MOS gates in the memory devices if the package were stressed sufficiently or if stress

in the package were released) and conducting lines on the IC or package which would oxidize rapidly if the package were opened in the air. These latter protection means are also symbolized by 5 in Fig 1.

The software for the arbitrator is contained in the PROM 12. The other memory in the arbitrator is the RAM 10. A principle use of this memory is to serve as temporary storage during calculation of the digital signature. The non-volatile part of RAM 10 maintains a record of any occasions when the clock was stopped and restarted.

The real-time clock 13 supplies the time which is appended to the input arbitrator ID. The power supply to the clock is a trickle-charged battery. The battery is to be accessible from outside the arbitrator 3 so that it can be replaced in the power-up state without affecting the clock 13. This results in the ability to maintain steady non-stop power to the clock for an indefinitely long time. The clock time is originally set at the factory.

The encryption device 14 is used to compute a digital signature on the time plus the arbitrator ID (signature data) using RSA public key techniques. Appropriate references to this subject may be found in the paper by Haber and Stornetta referred to above.

During power-up the I/O circuit 8 comes up with its input ports disabled. This ensures that the arbitrator 3 is isolated and that it is not possible to seize control of the arbitrator 3 during power-up. After power up the microcontroller 11 is in control and effectively isolates the arbitrator.

In the preferred mode of operation the microcontroller 11 monitors the I/O circuit 8. When a request for authenticated time is detected, the microcontroller 11 inputs a 64 bit random number supplied by the user, the correct time is retrieved from the real-time clock 13 and appended to the

random number, the arbitrator ID is appended, and the digital signature is computed on the combination. Then the random number, time, ID, and signature are presented for output to the I/O circuit 8 under control of the microcontroller 11.

Should the power, or system diagnostics, of the clock 13 or of other elements of the arbitrator 3 fail in such a way as to cast doubt on the integrity of the clock or of other elements of the arbitrator 3, the microcontroller 11 will store a permanent record of this fact in the non-volatile part of RAM 12, and respond to subsequent requests from the users with a default message indicating failure until the clock 13 has been reset, which is possible in this embodiment. (A simpler and more secure, but less flexible embodiment would not permit resetting. This could be ensured by setting a bit in the non-volatile part of RAM 12). If, as above the clock or other element of the arbitrator has failed, so long as power has been restored or is otherwise available to the clock 13, the microcontroller 11 will monitor the I/O circuit 8 for a command to reset the clock 13. Upon receiving such a command it will check that the clock has stopped, prompt for a password, required to provide flexible access control of all system operations, check that the new start time is later than the previous stop time, stored in the non-volatile part of RAM 12, perform other system diagnostics, and restart normal operations of the arbitrator if all checks are positive. The stop and start times are to be permanent records and are to be accessible for reading out at any time, also under password access control. Should the non-volatile part of RAM 12 be filled by a series of stops and starts, the system could no longer be used.

To use this device to ensure that a computer could not be booted with incorrect time, a critical element of the computer, in this embodiment the CPU chip, would be sealed, using means such as discussed above, with the public key and a random number generator which generates a different 64-bit number as an

authenticating signal each time it is called by using a secret key to encrypt a number which is incremented with each boot and which is stored in non-volatile RAM. Upon booting the chip would generate the 64-bit random number and send it to the arbitrator. Only if a signature was returned verifying the random number (which the arbitrator added to its ID before the signature was computed) and the expected arbitrator ID, would the returned time (checked to be later than the previous stop time) be used to set the computer system clock. Otherwise the CPU would refuse to boot.

No other signals presented to the I/O 8 constitute valid commands to the microcontroller 11, so that it is impossible for the user of the arbitrator 3 to, e.g., reset the clock to an earlier time or to detect the value of the secret key.

It may not be necessary to add the notary ID to the time, since in many applications the secret key will be unique, and successful decryption of the signature will identify the notary. However, for those cases where the keys are not unique, or simply for reasons of convenience and simplicity, it will likely usually be useful to add the notary ID.

A few modifications of the system described above to supply authenticated time are needed to provide a system (2) which will provide authentication for a digital document of the user ID, text (or other digital data), user sequence number, time, and notary ID and sequence number.

In this case, instead of simply presenting a request for authenticated time at the I/O circuit 8, the user presents a message comprising the user's public key digital signature, the user's document sequence number, and the text itself.

The microcontroller then uses the encryption circuit 14 to compute a hash over the input text and to append to the hash and the other data the internal time, the

notary ID, and the notary sequence number, resulting in the signature data. Naturally the details of the hash computation must be known to any user or verifier. Next, a digital signature is computed over the signature data using a secret key and the signature is returned to the I/O 8.

In a second process, the microcontroller will also, before hashing is performed, parse the portions of the input text indicated by the user to be simple text and reduce it to a standard format, in this embodiment a format in which only ascii characters on a standard keyboard are considered, tabs and new lines are ignored, and in which there is only a single space between each word. This format is more invariant under several forms of transcription and thus copies are more easily verified by recomputation of the digital signature, as discussed above. A signature is then also computed and returned in which only the hash of this transformed version of the text is in the signature data, together with the user signature and sequence number, the time, notary ID, and notary sequence number.

The notary sequence number might also well be computed and appended to the time before the signature was computed in the first aspect of the invention where the only function of the notary is to supply authenticated time. If users of the notary could examine this sequence number they might detect if attempts were being made to deduce the secret key using plain text attack using repeated requests for authenticated time.

Although these embodiments have been revealed in terms of the use of a public key encryption system with a single secret key, more complex systems could use multiple keys and other secret encryption data kept inaccessible within the notary to implement other signature methods both public and private.

Two aspects of the invention have thus been revealed: (1) A device and means for providing authenticated time to users, and for using such device and means

to ensure that computers cannot be booted up without setting their clocks to an authenticated time, and (2) A device and means for authenticating digital documents with respect to user, user sequence number, text, date, notary, and notary sequence number.

The foregoing descriptions of the preferred embodiments of the two aspects of the invention have been presented for the purposes of illustration and description. They are not intended to be exhaustive or to limit the inventions to the precise forms disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto.

What is claimed is:

(1) A sealed source of authenticated time, here called a notary, comprising a clock, computing means, and encryption means which performs operations comprising: receiving requests for authenticated time, retrieving the time from said clock, computing, using encryption data inaccessible from outside said notary, a notary digital signature on signature data comprising said time and returning said time and said notary digital signature to the user.

(2) The notary of claim (1) in which said notary further comprises means to receive an authenticating signal and to compute said notary digital signature over signature data comprising said time and said authentication signal.

(3) The notary of claim (1) in which said notary further comprises means to ensure non-stop power to said clock.

(4) The notary of claim (1) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said time and said notary digital signature.

(5) The notary of claim (1) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said atime and said notary digital signature, and that said clock may be subsequently reset and said notary restarted, and a permanent record of said failures be kept in said notary, and said permanent record be accessible from outside said notary, and that all said actions are under a system of access control.

(6) The notary of claim (2) in which said notary further comprises means to ensure non-stop power to said clock.

(7) The notary of claim (2) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said time and said notary digital signature.

(8) The notary of claim (2) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said atime and said notary digital signature, and that said clock may be subsequently reset and said notary restarted, and a permanent record of said failures be kept in said notary, and said permanent record be accessible from outside said notary, and that all said actions are under a system of access control.

(9) The notary of claim (3) in which said notary further comprises means to ensure that should power to said clock fail, or should said clock fail diagnostics, that a default message is returned and that said notary will no longer return said time and said notary digital signature.

(10) The notary of claim (3) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said atime and said notary digital signature, and that said clock may be subsequently reset and said notary restarted, and a permanent record of said failures be kept in said notary, and said permanent record be accessible from outside said notary, and that all said actions are under a system of access control.

(11) The notary of claim (6) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail

diagnostics, that a default message is returned and that said notary will no longer return said time and said notary digital signature.

(12) The notary of claim (6) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said atime and said notary digital signature, and that said clock may be subsequently reset and said notary restarted, and a permanent record of said failures be kept in said notary, and said permanent record be accessible from outside said notary, and that all said actions are under a system of access control.

(13) In claims 2, 6, 7, 8, 11, 12 said notary communicating with a remote computer system comprising means to generate said authenticating signal sealed with a critical element of said remote computer system; said means generating said authenticating signal when said remote computer system is booting, and said remote computer system using said authenticated time to initiate the system clock of said remote computer system.

(14) A sealed device, here called a notary, for time stamping and authenticating digital data, comprising a clock, computing means, and encryption means, said notary performing operations comprising: receiving requests for time stamping and digital data authentication, retrieving the time from said clock, computing, using encryption data inaccessible from outside said notary, a notary digital signature over signature data comprising said time and said digital data, and returning said time and said notary digital signature.

(15) The notary of claim (14) in which said notary further comprises means to ensure non-stop power to said clock.

(16) The notary of claim (14) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said time and said notary digital signature.

(17) The notary of claim (14) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail diagnostics, that a default message is returned and that said notary will no longer return said atime and said notary digital signature, and that said clock may be subsequently reset and said notary restarted, and a permanent record of said failures be kept in said notary, and said permanent record be accessible from outside said notary, and that all said actions are under a system of access control.

(18) The notary of claim (14) in which said notary further comprises means to parse said digital data and transform said digital data to a standard format which is more invariant under transcription, and to compute said notary digital signature using said transformed digital data in place of said untransformed digital data.

(19) The notary of claim (14) in which said notary further comprises means to receive a user digital signature and in which said signature data includes said time, said digital data, and said user digital signature.

(20) The notary of claim (14) in which said notary further comprises means to receive a user sequence number and in which said signature data includes said time, said digital data, and said user sequence number.

(21) The notary of claim (15) in which said notary further comprises means to ensure that should power to said clock fail, or should said notary fail

diagnostics, that a default message is returned and that said notary will no longer return said time and said notary digital signature.

(22) The notary of claim (15) in which said notary further comprises means to ensure that should power to said clock fail, or should said clock fail system diagnostics, that a default message is returned to the user, and that said notary will not time stamp and authenticate digital documents, but in which said clock may be subsequently reset and the notary restarted, and a permanent record of the stop and start kept in said notary, and in which said permanent records are accessible from outside the notary, and that all said actions are under a system of access control.

(23) The notary of claim (15) in which said notary further comprises means to parse said digital data and transform said digital data to a standard format which is more invariant under transcription, and to compute said notary digital signature using said transformed digital data in place of said untransformed digital data.

(24) The notary of claim (15) in which said notary further comprises means to receive a user digital signature and in which said signature data includes said time, said digital data, and said user digital signature.

(25) The notary of claim (15) in which said notary further comprises means to receive a user sequence number and in which said signature data includes said time, said digital data, and said user sequence number.

(26) The notary of claim (21) in which said notary further comprises means to parse said digital data and transform said digital data to a standard format which is more invariant under transcription, and to compute said notary digital signature using said transformed digital data in place of said untransformed digital data.

(27) The notary of claim (21) in which said notary further comprises means to receive a user digital signature and in which said signature data includes said time, said digital data, and said user digital signature.

(28) The notary of claim (21) in which said notary further comprises means to receive a user sequence number and in which said signature data includes said time, said digital data, and said user sequence number.

(29) The notary of claim (22) in which said notary further comprises means to parse said digital data and transform said digital data to a standard format which is more invariant under transcription, and to compute said notary digital signature using said transformed digital data in place of said untransformed digital data.

(30) The notary of claim (22) in which said notary further comprises means to receive a user digital signature and in which said signature data includes said time, said digital data, and said user digital signature.

(31) The notary of claim (22) in which said notary further comprises means to receive a user sequence number and in which said signature data includes said time, said digital data, and said user sequence number.

(32) The notary of claim (26) in which said notary further comprises means to receive a user digital signature and in which said signature data includes said time, said digital data, and said user digital signature.

(33) The notary of claim (26)in which said notary further comprises means to receive a user sequence number and in which said signature data includes said time, said digital data, and said user sequence number.

(34) The notary of claim (21) in which said notary further comprises means to accept a user digital signature and a user sequence number, and in which said signature data includes said time, said digital data, said user digital signature and said user sequence number.

(35) The notary of claim (29) in which said notary further comprises means to receive a user digital signature and in which said signature data includes said time, said digital data, and said user digital signature.

(36) The notary of claim (29) in which said notary further comprises means to receive a user sequence number and in which said signature data includes said time, said digital data, and said user sequence number.

(37) The notary of claim (22) in which said notary further comprises means to accept a user digital signature and a user sequence number, and in which said signature data includes said time, said digital data, said user digital signature and said user sequence number.

(38) The notary of claim (26) in which said notary further comprises means to accept a user digital signature and a user sequence number, and in which said signature data includes said time, said digital data, said user digital signature and said user sequence number.

(39) The notary of claim (29) in which said notary further comprises means to accept a user digital signature and a user sequence number, and in which said signature data includes said time, said digital data, said user digital signature and said user sequence number.

(40) In claims 1-39 said notary in which said notary's identification number is included in said signature data.

(41) In claims 1-40 said notary further comprises means to compute a notary sequence number and to include it in said signature data.

(42) In claims 1-41 said digital signature computed using public key means.

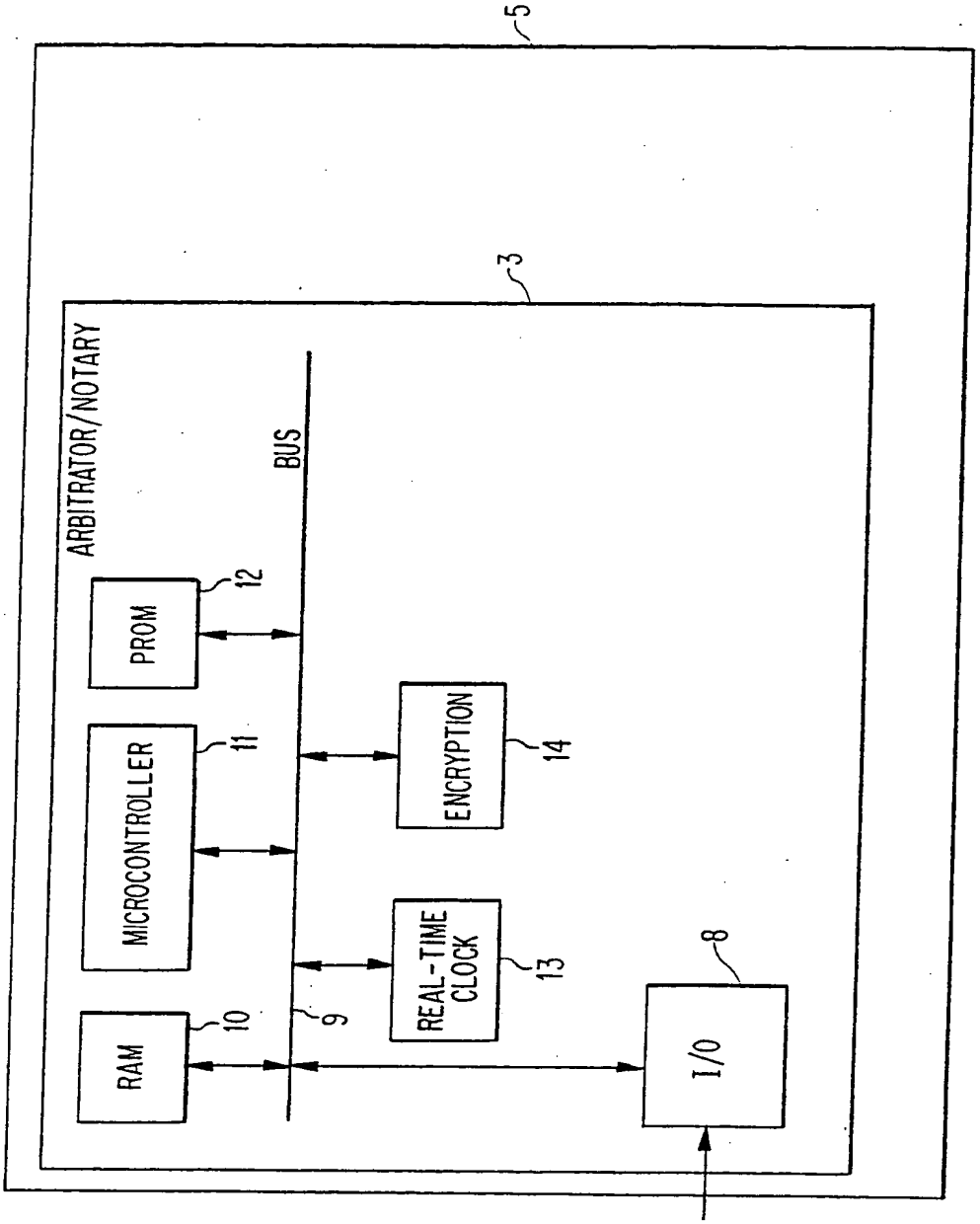


FIG. 1

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 91/09270

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl. 5 G06F12/14

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
Int.Cl. 5	G06F ; H04L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched[8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category °	Citation of Document,[11] with indication, where appropriate, of the relevant passages[12]	Relevant to Claim No.[13]
P,X	EP,A,0 422 757 (A.M. FISCHER) 17 April 1991 see the whole document	1,3-4,9
P,Y		14-16
P,A		2,6-7

P,Y	US,A,5 022 080 (R.T. DURST ET AL.) 4 June 1991 see abstract; claims; figures	14-16
P,A		1

A	PROC. ADVANCES IN CRYPTOLOGY - CRYPTO '90 AUG. 11-15, 1990 SANTA BARBARA, US pages 437 - 455; S. HABER ER AL.: 'How to time-stamp a digital document' cited in the application see abstract see page 442 - page 443	1-42

° Special categories of cited documents :[10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
23 MARCH 1992	10. 04. 92
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	PFITZINGER E.E.

Form PCT/ISA/210 (second sheet) (January 1985)

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. US 9109270 SA 55885

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 23/03/92
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0422757	17-04-91	US-A- 5001752	19-03-91
		AU-A- 5753190	18-04-91
		JP-A- 3185551	13-08-91
US-A-5022080	04-06-91	None	

EPO FORM P0479

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82